A Modification to the Self-Certified Group-Oriented Cryptosystem Without a Combiner

Indexing terms: Threshold Cryptography, Certified Public Keys

The authors propose a modified protocol which prevents the conspiracy attack developed by Susilo and Safavi-Naini on a self-certified group-oriented cryptosystem without combiner

Introduction: A society-oriented cryptographic system is a protocol which allows the distribution of the power of performing a cryptographic operation among a group of participants. Society-oriented cryptographic systems can be classified into two broad classes. If the membership of the group that performs the cryptographic operation is anonymous, then the society-oriented cryptographic system is called a *threshold cryptographic system* (even though the internal structure of the group is not a threshold structure). On the other hand, if the membership of the group is known, then the society-oriented cryptographic system is called a *group-oriented cryptographic system*.

A group-oriented cryptosystem is implemented by the sender. It is at the sender's discretion to create a subgroup $\mathcal{P} \subseteq \mathcal{U}$ of users for whom he encrypts a message. In addition, the sender determines a subgroup $\mathcal{A} \subseteq \mathcal{P}$ of intended receivers who are able to decrypt (collectively) a cryptogram generated by the sender. The sender also determines the access policy in the intended group.

An interesting class of all access structures is the threshold access structure. In a (t, n) group-oriented cryptosystem, collaboration of at least t participants is required to perform the group transformation. Two important issues in implementation of such cryptosystems are:

1. the sender needs to collect authenticated public keys of the intended receivers;

2. the combiner needs a secure channel to collect (privately) the partial results from collaborating participants.

In [1] the authors discussed relevant problems in implementation of such systems and proposed a (t, n) group-oriented cryptosystem that works with self-certified public keys and does not need the help of a combiner. In [2] Susilo and Safavi-Naini developed a conspiracy attack to the system, but they did not determine how to fix the problem. In this Letter, we show that the attack is not as straightforward as mentioned in [2], that is, the attack is applicable only in particular circumstances. We also present a small modification to the proposed scheme that prevents this type of attack and in the meantime preserves the main characteristics of the system. First we briefly review the *self-certified group-oriented cryptosystem without a combiner* and the *conspiracy attack*, then we present the modification to the system.

Self-certified group-oriented cryptosystem without a combiner: Let $\mathcal{U} = \{U_1, \ldots, U_\ell\}$ be the collection of all users in the system, and let (without loss of generality) $\mathcal{P} = \{U_1, \ldots, U_n\}$ $(n \leq \ell)$ be the intended group. As in all self-certified schemes, there exists a trusted authority who sets up the system.

Setup phase: The authority chooses:

(i) an integer N which is the product of two large distinct random primes p and q of almost the same size such that $p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are also prime integers,

(ii) a prime $F > N$,

(iii) a base $\alpha \neq 1$ of order $r = p'q'$ modulo N, and

(iv) a one-way hash function h, that outputs integers less than the minimum value of p' and q', that is, $h(m) < \min(p', q')$.

The authority makes α, h, F and N public, keeps r secret and discards p and q.

Key generation: Every legitimate user chooses his secret key x, computes the shadow $z = \alpha^x \pmod N$ and gives it to the authority. The authority first interrogates the user about his secret key. After the authority is convinced that the user knows the secret key, he generates the user's public key as

$$y = (z^{-1} - ID)^{ID^{-1}} \pmod N.$$

where $ID = h(I)$, and I corresponds to the user's identity (such as his name, his address, etc.)

Encryption: Suppose an individual wants to send a message $0 \leq m < N$ to the group $\mathcal{P} = \{U_1, \ldots, U_n\}$, such that cooperation of any t members of the group is sufficient to retrieve the message. The sender carries out the following:

- randomly chooses an integer k and computes $c = (\alpha^{-1})^k \pmod N$,
- randomly forms a polynomial $g(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1}$ in $GF(F)$ such that $g(0) = a_0 = \alpha^{h(m)} \pmod N$,
- computes for $i = 1, \ldots, n$

$$\begin{aligned} w_i &= y_i^{ID_i} + ID_i \pmod N \\ s_i &= w_i^k \pmod N \\ d_i &= g(s_i) \\ e_i &= m \cdot w_i^{h(m)} \pmod N \end{aligned}$$

and sends (t, c, d_i, e_i) to each U_i.

Decryption: Upon receiving the cryptogram, every group, $\mathcal{A} \subseteq \mathcal{P}$, of at least t intended receivers can cooperate to retrieve the plaintext message m. That is, each $U_i \in \mathcal{A}$ first calculates,

$$s_i = c^{x_i} \pmod{N},$$

and broadcasts the pair (d_i, s_i). When t values of such pairs are broadcasted, each U_i can recover $v = \alpha^{h(m)} \pmod{N}$, which allows him to compute the plaintext message as,

$$m = v^{x_i} e_i \pmod{N}.$$

Conspiracy attack: The Susilo *et al.* [2] attack is as follows:

Let U_i be a member of the group and let U_j, who conspires with U_i, be wanting to join the group. U_j chooses her secret key as $x_j = 2x_i$. Obviously, she is able to convince the trusted authority of the knowledge of the relevant secret key and thus she can obtain her public key as

$$y_j = (\alpha^{-2x_i} - ID_j)^{ID_j^{-1}} \pmod{N}.$$

Now when an encrypted message is broadcast, U_i and U_j can calculate (this is a simplified version of the calculation appearing in [2])

$$\frac{e_i \times e_i}{e_j} = \frac{m^2 \alpha^{-2x_i h(m)}}{m \alpha^{-2x_i h(m)}} = \frac{m^2}{m} = m \pmod{N}$$

which gives the message m without cooperating with other users.

We observe that the attack is effective if $t \geq 3$ (otherwise every two participants in the intended group are legitimate to decrypt the cryptogram) and both users U_i and U_j are in the intended group (we would like to draw the attention of the reader and authors of [2] to the fact that in group-oriented cryptographic systems the membership of the intended group is chosen by the sender –for more detail see [1]). However, we would like to acknowledge the authors of [2] for pointing out this possible weakness in the scheme.

The modification: Clearly the attack is applicable because the requirement was that the trusted authority must not know the users' secret key (see the original paper for precise discussion regarding this matter). In the following we show a small modification to the system that prevents this type of conspiracy attack and preserves the characteristics of the system. The modification is applied to the key generation phase.

The modified key generation: Every legitimate user, U_i, chooses his initial secret key x_i, computes the shadow $z = \alpha^{x_i} \pmod{N}$ and gives it to the authority. The

trusted authority chooses a random value r_i and gives it to U_i. The secret value of the user U_i is now $X_i = x_i + r_i$ and his shadow is

$$z_i = z \times \alpha^{r_i} = \alpha^{x_i + r_i} = \alpha^{X_i} \pmod{N}.$$

After the authority is convinced that the user knows the secret key, he generates the user's public key (the rest of the system remains at it was) as

$$y_i = (z_i^{-1} - ID_i)^{ID_i^{-1}} \pmod{N}.$$

Note that the trusted authority still has no knowledge about the secret value of any user and the system satisfies all requirements that have been discussed in the original paper. In fact, the purpose of adding a random number to the initial secret value chosen by users is to destroy possible structural relationships among the secret values of users. It is not difficult to see that the secret values of users now look like randomly chosen values and thus the conspiracy attack is no more applicable to the system.

H. Ghodosi *School of Information Technology, James Cook University, Townsville, 4811, Australia.*
S. Saeednia *Université Libre de Bruxelles, Département d'Informatique, CP 212, Boulevard du Triomphe, 1050 Bruxelles, Belgium.*

References

[1] S. Saeednia and H. Ghodosi, "A Self-Certified Group-Oriented Cryptosystem Without a Combiner," in *Proceedings of ACISP '99 –Australasian Conference on Information Security and Privacy* (J. Pieprzyk, R. Safavi-Naini, and J. Seberry, eds.), vol. 1587 of *Lecture Notes in Computer Science*, pp. 192–201, Springer-Verlag (Berlin), 1999.

[2] W. Susilo and R. Safavi-Naini, "Remark on self-certified group-oriented cryptosystem without combiner," *Electronics Letters*, vol. 35, pp. 1539–1540, Sept. 1999.